PCT / IB 99 / 01323

16. 08. 99

Europäisches Patentamt | Eur pean Patent Office | Office eur péen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

98401778.0

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

Arlette Fiedler

A. Fiedler

DEN HAAG, DEN
THE HAGUE,
LA HAYE, LE 14/07/99

Eur päisches Patentamt
Eur pean Patent Office
Office eur péen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.: 98401778.0
Demande n°:

Anmeldetag:
Date of filing: 15/07/98
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
CANAL+ Société Anonyme
75711 Paris Cedex 15
FRANCE

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Method and apparatus for secure communication of information between a decoder device and a recorder device

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat:	Tag:	Aktenzeichen:
State:	Date:	File no.
Pays:	Date:	Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
H04N7/167, H04L29/06

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

METHOD AND APPARATUS FOR SECURE COMMUNICATION OF INFORMATION BETWEEN A DECODER DEVICE AND A RECORDER DEVICE

The present invention relates to a method and apparatus for secure communication of information between a decoder device and a recorder device.

The present invention is particularly applicable to the field of digital television, where scrambled audiovisual information is broadcast typically by satellite to a number of subscribers, each subscriber possessing a decoder or integrated receiver/decoder (IRD) capable of descrambling the transmitted program for subsequent viewing.

In a typical system, scrambled digital data is transmitted together with a control word for descrambling of the digital data, the control word itself being encrypted by an exploitation key and transmitted in encrypted form. A decoder receives the scrambled digital data and encrypted control word which uses an equivalent of the exploitation key to decrypt the encrypted control word and thereafter descramble the transmitted data. A paid-up subscriber will receive periodically the exploitation key necessary to decrypt the encrypted control word so as to permit viewing of a particular program. As part of the subscription, a subscriber may also have the right to record a broadcast for his own use.

A particular problem associated with data transmitted in a digital system lies in its ease of reproduction with no loss of quality. Where a descrambled program is passed via an analogue link (e.g. the « Peritel » link) for viewing and recording by a standard VCR the quality remains no greater than that associated with a standard analogue cassette recording.

By way of contrast, any descrambled digital data passed by a direct digital link to one of the new generation of digital recording devices (for example, a DVHS or DVD recorder) will be of the same quality as th originally transmitted program and may thus be reproduced any number of times without any degradation of image or sound quality. There is therefore a considerable risk that recorded descrambled data will be used as a master recording to make pirate copies.

French Patent Application 95 03859 shows one way of overcoming this problem. In this system, descrambled digital data is never recorded directly on the digital recording medium. Instead, the decoder described in this application forwards the data for recordal on the support medium in its scrambled form. The control word necessary to descramble the data is re-encrypted by means of another key and stored on the recording support with the scrambled data. This new key is known only to the receiver/decoder and replaces the exploitation key needed to obtain the control word for viewing of the program.

The advantage of such a system is that the data is never stored in a « clear » form and cannot be viewed without possession of the new key, stored in the decoder. The system also possesses the advantage that, since the exploitation key changes on a monthly basis, the use of a key chosen by the decoder to re-encrypt the control word registered on the digital tape means that the decoder will still be able to decrypt the control word recorded on the tape even after the end of a subscription month.

The disadvantage of the system proposed in this previous patent application is that the recording can only be viewed in conjunction with that particular decoder. If that decoder breaks down, or is replaced, the recording can no longer be replayed. Equally, it is not possible to play the recording directly in a digital recorder without connecting the decoder in the system.

In order to enable the decoder and recorder to function more effectively it is desired to provide a securised or encrypted communication link between the devices. As will be appreciated from the above description, the interaction of the decoder and recorder may lead to problems, for example, where scrambled transmissions are recorded but where only the decoder possesses the information needed to decrypt such transmissions. The implementation of a secure link between the devices can be used to enable information needed to prepare or play a recording to be passed freely between the devices.

According to the present invention there is providing a method of providing secure communication of information between a decoder device and a recorder device and characterised in that a first one of the devices communicates to the second device a certificate comprising a device public key encrypted

by a management private key, the second device decrypting the certificate using an equivalent management public key and thereafter using the device public key to encrypt information sent to the first device, the first device using an equivalent device private key to decrypt the information.

In such a method, the first device initiating the communication is personalised with a certificate generated by a management private key. The management private key is held in secret by the source responsible for this device (e.g. a recorder device manufacturer) and may not be derived from the information stored in the certificate. The communication of such a certificate therefore provides the second device with a level of assurance concerning the identity and origin of the device initiating the communication.

In addition, the information encrypted by the device public key held by the second device may only be decrypted by the equivalent private key held by the first device thereby enabling the second device to communicate in confidence information to the first device. As will be described below, this information may thereafter be used to set up a secure bi-directional link.

Preferably, prior to the communication of the first device certificate, the first device communicates to the second device a system certificate comprising the management public key encrypted by a system private key, the second device decrypting the system certificate using a system public key so as to obtain the management public key used thereafter to decrypt the device certificate.

The private system key may be held in secret by, for example, the source of the second device (e.g. a broadcast system manager responsible for the decoder). A system certificate will only be issued in the event that the second device source is sure of the integrity of security at the first device source, that is, that the second device source is sure that the management private key is only known to by the first device source and that the necessary measures have been put in place to keep this key secret.

As will be understood, the second device source need only know the public management key of the first device source in order to generate a system certificate and neither party needs to share its private encryption keys in carrying out these certifying operations.

Advantageously, the device private/public key pair are uniquely associated with the first device. This ensures complete security of encrypted messages transmitted to the first device. Further advantageously, the management private/public key pair are uniquely associated with the source of the first device and the system private/public key pair (if present) are uniquely associated with the source of the second device.

As will be appreciated, although the use of unique keys enables an increased level of security, it may be decided in some cases to use non-unique keys. For example, in the case of high volume of production of first devices, certain of these devices may share the same device private key if such devices are distributed in different territories, since the security risk associated with such duplication is relatively low.

Preferably, the encrypted information sent by the second device comprises a session key, in particular, a session key generated by the second device and usable in conjunction with a symmetric encryption algorithm. This key, which may be generated at the initiation of a recording session can thereafter be used for bi-directional communication of information between the first and second devices.

In an alternative embodiment, a session key pair corresponding to a private/public key pair of an asymmetric algorithm may be used.

The advantage of a changeable session key lies in the increased level of security that such a key provides as well as the possibility of secure bi-directional communication that it enables if a symmetric session key is chosen. Other embodiments are nevertheless possible, for example, in which information associated with a recording operation may be directly encrypted using the device public key held by the second device.

In one embodiment, the session key is used by the decoder device to encrypt control word information subsequently communicated to the recorder device. In such an embodiment, the recorder device may

decrypt the control word information using the equivalent session key and thereafter re-encrypt the control word information using a recording encryption key, the re-encrypted control word information being stored by the recorder on a recording support medium together with the scrambled transmission data associated with that control word information.

The encryption of control word information using a recording key held by the recorder device enables the recorder device to replay at any time a recorded scrambled transmission independently of the decoder device originally used to receive and forward the transmission.

Advantageously, the recorder device communicates to the decoder device a copy of the recording encryption key. This may be conveniently encrypted by the session key prior to communication. This copy may thereafter be decrypted by the decoder and a back-up copy of the recording key stored in the decoder.

As will be understood, the secure communication link may be used to convey many different types of information. In particular, whilst the above embodiments discuss the use of a session key in the encryption and communication of control word information for use in a recording operation, other embodiments are possible. For example, audio and/or visual data to be recorded may be directly encrypted by the decoder using a session key and communicated to the recorder for decryption and subsequent re-encryption prior to recordal.

Other embodiments may use the secure communication link to transfer, for example, decoder exploitation keys to the recorder device such that the recorder device can carry out all operations to decrypt control word information and/or descramble a transmission prior to its recordal in a re-encrypted or rescrambled form on a recording support medium.

Whilst the above description has described encryption and decryption operations in relation to a decoder device or recorder device it is to be understood that these operations and, in particular the keys needed in such operations, need not necessarily handled by elements permanently integrated in the devices themselves.

In particular, in a preferred embodiment, the recorder and/or decoder device may further comprise a portable security module associated with that device and used to carry out some or all of the encryption or decryption steps described above.

Such portable security devices can take any convenient form depending on the physical size and characteristics of the decoder or recorder. For example, a smart card or PCMCIA type card may be used with a decoder and a SIM card or similar with a recorder.

In a particularly preferred embodiment of the invention, the first device corresponds to a recorder device and the second device to a decoder device. In such a system the decoder system manager will have ultimate control, for example, over generation of system certificates issued to recorder manufacturers. Similarly communication will be initiated by the recorder, the decoder only communicating an encrypted message containing the information that will be needed to set up a bi-directional communication in the event that the recorder has communicated correct system and/or management certificates.

The present invention is particularly but not exclusively adapted for use with a digital television transmission system in which the decoder device is adapted to receive a digital television transmission.

The present invention has been described above in relation to a method of recording transmitted digital data. The invention equally extends to a decoder device and/or a recorder device adapted for use in such a method and one or more portable security modules adapted for use in such a method.

The terms "scrambled" and "encrypted" and "control word" and "key" have been used at various parts in the text for the purpose of clarity of language. However, it will be understood that no fundamental distinction is to be made between "scrambled data" and "encrypted data" or between a "control word" and a "key". Similarly, the term "equivalent key" is used to refer to a key adapted to decrypt data encrypted by a first mentioned key, or vice versa.

Suitable algorithms for use in this invention for generating private/public keys may include RSA or Diffie-Hellman, and suitable symmetric key algorithms may include DES type algorithms, for example. However, unless obligatory in view of the context or unless otherwise specified, no general distinction is made between keys associated with symmetric algorithms and those associated with public/private algorithms.

The term "receiver/decoder", "decoder" or "decoder device" as used herein may connote a receiver for receiving either encoded or non-encoded signals, for example, television and/or radio signals, which may be broadcast or transmitted by some other means. The term may also connote a decoder for decoding received signals. Embodiments of such decoders may also include a decoder integral with the receiver for decoding the received signals, for example, in a "set-top box", a decoder functioning in combination with a physically separate receiver, or such a decoder including additional functions, such as a web browser or a video recorder or a television. In a similar manner, the term "recorder" or "recorder device" may cover and digital recording and/or playback devices either in isolation or integrated with other electronic devices.

In particular, whilst the invention is particularly convenient where the decoder and recorder are physically separate, the invention may equally be used in a combination recorder/decoder apparatus to provide, for example, a secure bus link between the recorder and decoder devices within the combined apparatus.

As used herein, the term "digital transmission system" includes any transmission system for transmitting or broadcasting for example primarily audiovisual or multimedia digital data. Whilst the present invention is particularly applicable to a broadcast digital television system, the invention may also be applicable to a fixed telecommunications network for multimedia internet applications, to a closed circuit television, and so on.

As used herein, the term "digital television system" includes for example any satellite, terrestrial, cable and other system.

There will now be described, by way of example only, a number of embodiments of the invention, with reference to the following figures, in which:

Figure 1 shows the overall architecture of a digital TV system according to this embodiment;

Figure 2 shows the architecture of the conditional access system of Figure 1;

Figure 3 shows the encryption levels in the conditional access system;

Figure 4 shows the layout of a decoder and digital recording device according to this embodiment; and

Figure 5 shows the steps associated with the personalisation of decoder and recorder security modules and with the subsequent operations carried out to set up a secure communication link between the devices.

An overview of a digital television broadcast and reception system 1 is shown in Figure 1. The invention includes a mostly conventional digital television system 2 which uses the MPEG-2 compression system to transmit compressed digital signals. In more detail, MPEG-2 compressor 3 in a broadcast centre receives a digital signal stream (for example a stream of audio or video signals). The compressor 3 is connected to a multiplexer and scrambler 4 by linkage 5. The multiplexer 4 receives a plurality of further input signals, assembles one or more transport streams and transmits compressed digital signals to a transmitter 6 of the broadcast centre via linkage 7, which can of course take a wide variety of forms including telecom links.

The transmitter 6 transmits electromagnetic signals via uplink 8 towards a satellite transponder 9, where they are electronically processed and broadcast via a notional downlink 10 to earth receiver 11, conventionally in the form of a dish owned or rented by the end user. The signals received by receiver 11 are transmitted to an integrated receiver/decoder 12 owned or rented by the end user and connected to

the end user's television set 13. The receiver/decoder 12 decodes the compressed MPEG-2 signal into a television signal for the television set 13.

A conditional access system 20 is connected to the multiplexer 4 and the receiver/decoder 12, and is located partly in the broadcast centre and partly in the decoder. It enables the end user to access digital television broadcasts from one or more broadcast suppliers. A smartcard, capable of decrypting messages relating to commercial offers (that is, one or several television programmes sold by the broadcast supplier), can be inserted into the receiver/decoder 12. Using the decoder 12 and smartcard, the end user may purchase events in either a subscription mode or a pay-per-view mode.

An interactive system 17, also connected to the multiplexer 4 and the receiver/decoder 12 and again located partly in the broadcast centre and partly in the decoder, may be provided to enable the end user to interact with various applications via a modemmed back channel 16.

The conditional access system 20 will now be described in more detail. With reference to Figure 2, in overview the conditional access system 20 includes a Subscriber Authorization System (SAS) 21. The SAS 21 is connected to one or more Subscriber Management Systems (SMS) 22, one SMS for each broadcast supplier, by a respective TCP-IP linkage 23 (although other types of linkage could alternatively be used). Alternatively, one SMS could be shared between two broadcast suppliers, or one supplier could use two SMSs, and so on.

First encrypting units in the form of ciphering units 24 utilising "mother" smartcards 25 are connected to the SAS by linkage 26. Second encrypting units again in the form of ciphering units 27 utilising mother smartcards 28 are connected to the multiplexer 4 by linkage 29. The receiver/decoder 12 receives a portable security module, for example in the form of "daughter" smartcard 30. It is connected directly to the SAS 21 by Communications Servers 31 via the modemmed back channel 16. The SAS sends, amongst other things, subscription rights to the daughter smartcard on request.

The smartcards contain the secrets of one or more commercial operators. The "mother" smartcard encrypts different kinds of messages and the "daughter" smartcards decrypt the messages, if they have the rights to do so.

The first and second ciphering units 24 and 27 comprise a rack, an electronic VME card with software stored on an EEPROM, up to 20 electronic cards and one smartcard 25 and 28 respectively, for each electronic card, one card 28 for encrypting the ECMs and one card 25 for encrypting the EMMs.

The operation of the conditional access system 20 of the digital television system will now be described in more detail with reference to the various components of the television system 2 and the conditional access system 20.

Multiplexer and Scrambler

With reference to Figures 1 and 2, in the broadcast centre, the digital audio or video signal is first compressed (or bit rate reduced), using the MPEG-2 compressor 3. This compressed signal is then transmitted to the multiplexer and scrambler 4 via the linkage 5 in order to be multiplexed with other data, such as other compressed data.

The scrambler generates a control word used in the scrambling process and included in the MPEG-2 stream in the multiplexer. The control word is generated internally and enables the end user's integrated receiver/decoder 12 to descramble the programme.

Access criteria, indicating how the programme is commercialised, are also added to the MPEG-2 stream. The programme may be commercialised in either one of a number of "subscription" modes and/or one of a number of "Pay Per View" (PPV) modes or events. In the subscription mode, the end user subscribes to one or more commercial offers, or "bouquets", thus getting the rights to watch every channel inside those bouquets.

In the Pay Per View mode, the end user is provided with the capability to purchase events as he wishes. This can be achieved by either pre-booking the event in advance ("pre-book mode"), or by purchasing the event as soon as it is broadcast ("impulse mode"). In the preferred embodiment, all users are subscribers, whether or not they watch in subscription or PPV mode, but of course PPV viewers need not necessarily be subscribers.

Entitlement Control Messages

Both the control word and the access criteria are used to build an Entitlement Control Message (ECM). This is a message sent in relation with a scrambled program; the message contains a control word (which allows for the descrambling of the program) and the access criteria of the broadcast program. The access criteria and control word are transmitted to the second encrypting unit 27 via the linkage 29. In this unit, an ECM is generated, encrypted and transmitted on to the multiplexer and scrambler 4. During a broadcast transmission, the control word typically changes every few seconds, and so ECMs are also periodically transmitted to enable the changing control word to be descrambled. For redundancy purposes, each ECM typically includes two control words; the present control word and the next control word.

Each service broadcast by a broadcast supplier in a data stream comprises a number of distinct components; for example a television programme includes a video component, an audio component, a sub-title component and so on. Each of these components of a service is individually scrambled and encrypted for subsequent broadcast to the transponder 9. In respect of each scrambled component of the service, a separate ECM is required. Alternatively, a single ECM may be required for all of the scrambled components of a service. Multiple ECMs are also generated in the case where multiple conditional access systems control access to the same transmitted program.

Entitlement Management Messages (EMMs)

The EMM is a message dedicated to an individual end user (subscriber), or a group of end users. Each group may contain a given number of end users. This organisation as a group aims at optimising the bandwidth; that is, access to one group can permit the reaching of a great number of end users.

Various specific types of EMM can be used. Individual EMMs are dedicated to individual subscribers, and are typically used in the provision of Pay Per View services; these contain the group identifier and the position of the subscriber in that group.

Group subscription EMMs are dedicated to groups of, say, 256 individual users, and are typically used in the administration of some subscription services. This EMM has a group identifier and a subscribers' group bitmap.

Audience EMMs are dedicated to entire audiences, and might for example be used by a particular operator to provide certain free services. An "audience" is the totality of subscribers having smartcards which bear the same conditional access system identifier (CA ID). Finally, a "unique" EMM is addressed to the unique identifier of the smartcard.

EMMs may be generated by the various operators to control access to rights associated with the programs transmitted by the operators as outlined above. EMMs may also be generated by the conditional access system manager to configure aspects of the conditional access system in general.

Programme Transmission

The multiplexer 4 receives electrical signals comprising encrypted EMMs from the SAS 21, encrypted ECMs from the second encrypting unit 27 and compressed programmes from the compressor 3. The multiplexer 4 scrambles the programmes and sends the scrambled programmes, the encrypted EMMs and the encrypted ECMs to a transmitter 6 of the broadcast centre via the linkage 7. The transmitter 6 transmits electromagnetic signals towards the satellite transponder 9 via uplink 8.

Programm Reception

The satellite transponder 9 receives and processes the electromagnetic signals transmitted by the transmitter 6 and transmits the signals on to the earth receiver 11, conventionally in the form of a dish owned or rented by the end user, via downlink 10. The signals received by receiver 11 are transmitted to the integrated receiver/decoder 12 owned or rented by the end user and connected to the end user's television set 13. The receiver/decoder 12 demultiplexes the signals to obtain scrambled programmes with encrypted EMMs and encrypted ECMs.

If the programme is not scrambled, that is, no ECM has been transmitted with the MPEG-2 stream, the receiver/decoder 12 decompresses the data and transforms the signal into a video signal for transmission to television set 13.

If the programme is scrambled, the receiver/decoder 12 extracts the corresponding ECM from the MPEG-2 stream and passes the ECM to the "daughter" smartcard 30 of the end user. This slots into a housing in the receiver/decoder 12. The daughter smartcard 30 controls whether the end user has the right to decrypt the ECM and to access the programme. If not, a negative status is passed to the receiver/decoder 12 to indicate that the programme cannot be descrambled. If the end user does have the rights, the ECM is decrypted and the control word extracted. The decoder 12 can then descramble the programme using this control word. The MPEG-2 stream is decompressed and translated into a video signal for onward transmission to television set 13.

Subscriber Management System (SMS)

A Subscriber Management System (SMS) 22 includes a database 32 which manages, amongst others, all of the end user files, commercial offers, subscriptions, PPV details, and data regarding end user consumption and authorization. The SMS may be physically remote from the SAS.

Each SMS 22 transmits messages to the SAS 21 via respective linkage 23 which imply modifications to or creations of Entitlement Management Messages (EMMs) to be transmitted to end users.

The SMS 22 also transmits messages to the SAS 21 which imply no modifications or creations of EMMs but imply only a change in an end user's state (relating to the authorization granted to the end user when ordering products or to the amount that the end user will be charged).

The SAS 21 sends messages (typically requesting information such as call-back information or billing information) to the SMS 22, so that it will be apparent that communication between the two is two-way.

Subscriber Authorization System (SAS)

The messages generated by the SMS 22 are passed via linkage 23 to the Subscriber Authorization System (SAS) 21, which in turn generates messages acknowledging receipt of the messages generated by the SMS 21 and passes these acknowledgements to the SMS 22.

In overview the SAS comprises a Subscription Chain area to give rights for subscription mode and to renew the rights automatically each month, a Pay Per View Chain area to give rights for PPV events, and an EMM Injector for passing EMMs created by the Subscription and PPV chain areas to the multiplexer and scrambler 4, and hence to feed the MPEG stream with EMMs. If other rights are to be granted, such as Pay Per File (PPF) rights in the case of downloading computer software to a user's Personal Computer, other similar areas are also provided.

One function of the SAS 21 is to manage the access rights to television programmes, available as commercial offers in subscription mode or sold as PPV events according to different modes of commercialisation (pre-book mode, impulse mode). The SAS 21, according to those rights and to information received from the SMS 22, generates EMMs for the subscriber.

The EMMs are passed to the Ciphering Unit (CU) 24 for ciphering with respect to the management and exploitation keys. The CU completes the signature on the EMM and passes the EMM back to a Message Generator (MG) in the SAS 21, where a header is added. The EMMs are passed to a Message Emitter (ME) as complete EMMs. The Message Generator determines the broadcast start and stop time and the rate of emission of the EMMs, and passes these as appropriate directions along with the EMMs to the

Message Emitter. The MG only generates a given EMM once; it is the ME which performs cyclic transmission of the EMMs.

On generation of an EMM, the MG assigns a unique identifier to the EMM. When the MG passes the EMM to the ME, it also passes the EMM ID. This enables identification of a particular EMM at both the MG and the ME.

In systems such as simulcrypt which are adapted to handle multiple conditional access systems e.g. associated with multiple operators, EMM streams associated with each conditional access system are generated separately and multiplexed together by the multiplexer 4 prior to transmission.

Encryption Levels of the Broadcast System

Referring now to Figure 3, a simplified outline of the encryption levels in a standard broadcast system will now be described. The stages of encryption associated with the broadcast of the digital data are shown at 41, the transmission channel (eg a satellite link as described above) at 42 and the stages of decryption at the receiver at 43.

The digital data N is scrambled by a control word CW before being transmitted to a multiplexer Mp for subsequent transmission. As will be seen from the lower part of Figure 3, the transmitted data includes an ECM comprising, inter alia, the control word CW as encrypted by an encrypter Ch1 controlled by a first encryption key Kex. At the receiver/decoder, the signal passes by a demultiplexer DMp and descrambler D before being passed to a television 13 for viewing. A decryption unit DCh1 also possessing the key Kex decrypts the ECM in the demultiplexed signal to obtain the control word CW subsequently used to descramble the signal.

For security reasons, the control word CW embedded in the encrypted ECM changes on average every 10 seconds or so. In contrast, the first encryption key Kex used by the receiver to decode the ECM is changed every month or so by means of an operator EMM. The encryption key Kex is encrypted by a second unit ChP using a personalised group key K1(GN). If the subscriber is one of

those chosen to receive an updated key Kex, a decryption unit DChP in the decoder security module will decrypt the message using its group key K1(GN) to obtain that month's key Kex.

The decryption units DChp and DCh1 and the associated keys are held on a security module associated with the decoder, in this case the smart card 30 provided to the subscriber and inserted in a smart card reader in the decoder. The keys may be generated, for example, according to any generally used symmetric key algorithm or in accordance with a customised symmetric key algorithm.

As will be described, different keys may be associated with different operators or broadcasters as well as with the conditional access system supplier. In the above description, a group key K1(GN) is held by the smart card associated with the decoder and used to decrypt EMM messages. In practice, different operators will have different subscriber unique keys K1 (Op1, GN1), K1 (Op2, GN2) etc. Each group key is generated by an operator and diversified by a value associated with the group to which the subscriber belongs.

Different memory zones in the smart card hold the keys for different operators. Each operator may also have a unique key associated solely with the smart card in question and an audience key for all subscribers to the services provided by that operator (see above).

In addition, a set of keys may also be held by the manager of the conditional access system. In particular, a given smart card may include a user specific key K0 (NS) and an audience key K1 (C), common to all smart cards. Whilst the operator keys are generally used to decode EMM messages associated with broadcast rights, the conditional access manager keys may be used to decrypt EMM messages associated with changes to conditional access system in general, as will be described below.

The above description of the system shown in Figure 3 relates to the implementation of access control in a broadcast system in which transmissions are descrambled by a decoder and displayed immediately. Referring to Figure 4, the elements of an access control system for recordal and replaying of scrambled transmission will now be described.

Decoder and Recorder Configuration

As before, a decoder 12 receives scrambled broadcast transmissions via a receiver 11. The decoder includes a portable security module 30, which may conveniently take the form of a smart card, but which may comprise any other suitable memory or microprocessor device. The decoder 12 includes a modem channel 16, for example, for communicating with servers handling conditional access information and is also adapted to pass descrambled audiovisual display information, e.g. via a Peritel link 53, to a television 13. The system additionally includes a digital recorder 50, such as a DVHS or DVD recorder, adapted to communicate with the decoder, for example, via an IEEE 1394 bus 51. The recorder 50 receives a digital recording support (not shown) on which information is recorded.

The recorder 50 is further adapted to function with a portable security module 52 containing, inter alia, the keys used to control access to the replaying of a recording. The portable security module may comprise any portable memory and/or microprocessor device as is conventionally known, such as a smart card, a PCMCIA card, a microprocessor key etc. In the present case, the portable security module 52 has been designated as a SIM card, as is known from the field of portable telephones.

The digital recorder 50 includes a direct link 54 to the display 13. In alternative realisations, digital audiovisual information may be passed from the recorder 50 to the decoder 12 prior to display. Equally, whilst the elements of decoder 12, recorder 50 and display 13 have been indicated separately, it is conceivable that some or all of these elements may be merged, for example, to provide a combined decoder/television set or combined decoder/recorder etc.

Similarly, whilst the invention will be discussed in relation to the recording of audiovisual broadcast information, it may also conveniently be applied, for example, to broadcast exclusive audio information subsequently recorded on a DAT or minidisc recorder or even a broadcast software application recorded on the hard disc of a computer.

Secure Communication between Decoder and Recorder

As set out in the introduction, it is known from prior art proposed systems to re-encrypt the control word associated with a scrambled transmission with a recording key and to store the re-encrypted control word on the recording support with the scrambled transmission. Unlike the exploitation key associated with encryption and decryption of the original transmission, the recording key may be an unchanging key associated with this particular recording so as to enable the recording to be played back at any time in the future.

As will be seen from the overview of Figure 4, in order to enable independence of the recording elements of the system from the decoder elements, it is necessary that the recording key be associated with the recorder 50, for example, by storing the key in a security module associated with the recorder such as the portable security module SIM card 52. Otherwise, if the key is permanently stored at decoder 12 or smart card 30 it will not be possible for a recorder to play back a recording in the absence of the decoder.

In order to do this it will be necessary to pass certain information between the decoder 12 and the recorder 50 along the link 51. This information may be, for example, decrypted control word information that may be then re-encrypted by use of a recording key at the digital recorder. Alternatively, control word information may be encrypted by a recording key generated by the decoder, this recording key then being sent to the recorder for storage.

In all cases it is necessary to ensure a securised link between the decoder and recorder. Unfortunately, the independence of activities between a broadcast system manager responsible for the decoder and a manufacturer of recording equipment responsible for the recorder may lead to a number of problems regarding the provision of encryption keys for this purpose.

For example, a broadcast operator may not place sufficient confidence in the integrity of security at the manufacturing site of a recorder to entrust the manufacturer with, for example, a secret symmetric

algorithm key needed by the recorder security module 52 to decrypt communications encrypted using the equivalent key held by the decoder security module 30.

Furthermore, the separation of activities may make it impractical to envisage a situation in which the recorder security module 52 is sent to a broadcast system manager for personalisation with the appropriate keys. For this reason, it is necessary to envisage a solution which allows the greatest independence of operation for the decoder and recorder.

Figure 5 shows in schematic form a method of setting up a secure communication link between the decoder and recorder security modules 30, 52 that overcomes these problems.

For the sake of clarity, all encryption/decryption operations using a public/private key algorithm are indicated by means of the symbol f_a in a hexagon, whilst all operations using a symmetric algorithm are indicated by the symbol f_s in an oval.

As shown in Figure 5, the recorder card 52 is prepared by the recorder manufacturer using a system certificate CtKeyRec shown at 70 that is communicated to the recorder manufacturer by the broadcast system manager. As is shown at 71, this certificate corresponds to a manufacturer public key KpubMan encrypted by a broadcaster system private key KpriSystem. The private key KpriSystem is unique to and held exclusively by the system manager and it is not possible to derive this key value from the certificate CtKeyRec even if the value KpubMan is known.

As will become clearer from the description below, the system certificate CtKeyRec which includes the manufacturer key KpubMan serves as a guarantee by the broadcast operator of the integrity of the security of the key system of the manufacturer and, notably, the validity of the key KpubMan. The certificate is generated once only. In this certifying operation, the manufacturer communicates the key KpubMan to the broadcast system manager, who encrypts the key KpubMan using the private key KpriSystem and returns the system certificate CtKeyRec. Thereafter, the manufacturer configures all recorder security modules to include the certificate CtKeyRec during the personalisation step of the recorder security modules.

The key KpubMan itself corresponds to a public key of a private/public key pair associated with the identity of and unique to the recorder manufacturer or source of the recorder. The corresponding private key KpriMan is held exclusively by the recorder manufacturer and is not known even to the broadcast system manager. The key KpriMan is itself used to generate a device certificate CtKeySIM shown at 72. This certificate, which is unique to the recorder security module, corresponds to a recorder security module key KpubSIM encrypted by the private manufacturer key KpriMan.

The key KpubSIM equally corresponds to a public key of a private/public key pair associated with the identity of and unique to the recorder device. This key and the corresponding private key KpriSIM are generated by the recorder manufacturer. As shown, the private key KpriSIM is stored in the recorder security module at 74, preferably at the moment of manufacture of the chip itself.

In the event that an encrypted communication is to be set up between the decoder and the recorder, for example, associated with the recording of a transmission received by the decoder, the system certificate CtKeyRec is transmitted from the recorder security module 52 to the decoder security module 30 as shown at 76.

The decoder security module 30 includes the broadcast system public key KpubSystem shown at 75 and stored in the card 30 during personalisation by the broadcast system manager. Using the system key KpubSystem, the decoder security module decrypts at 77 the certificate CtKeyRec in order to obtain the manufacturer public key KpubMan.

In the case of a security breach associated with the recorder source, the security module 30 can be programmed to reject certain manufacturer public key values obtained after the decryption step 77. Otherwise, the key KpubMan is stored at 78 and will be used in the next decryption steps.

As shown at 79, the recorder security module 52 then communicates the device certificate CtKeySIM, unique to that recorder security module, to the decoder security module 30. Using the manufacturer

public key KpubMan, the decoder security module 30 decrypts at 80 the recorder security module public key KpubSIM.

This public key is stored at 81 in the decoder security module 30 and is then used in the encryption and communication of a session key value. This session key value, which in this example corresponds to a random number value usable by a symmetric encryption/decryption algorithm, is generated at 82, encrypted at 83 by the recorder security module public key KpubSIM and then communicated to the recorder security module at 84.

As will be understood, in view of the nature of public/private key algorithms, this encrypted message may only be decrypted using the unique private key KpriSIM stored at 74 in the recorder security module. Decryption of the message at 85 leads to the extraction of the session key at 86.

Thereafter, each security module 30, 52 will possess a copy of the symmetric session key at 87, 88 for use in encryption and decryption of bi-directional messages. As mentioned above, the session key is used in combination with a symmetric algorithm and equal security is provided for messages in either direction. Other embodiments not requiring bi-directional communication and using an asymmetric algorithm may be envisaged.

As shown in Figure 5, the session key is used in this embodiment to communicate control word information from the decoder to the recorder. In particular, an ECM message 89 associated with the scrambled transmission is received and decrypted by the decoder security module to obtain the clear value of the control word 90 together with any other information contained therein. This control word is then re-encrypted at 91 using the session key stored at 87, and the resulting encrypted message communicated at 92 to the recorder security module 52.

Using the session key stored at 88, the recorder security module decrypts the message at 93 to obtain the clear value of the control word at 94. The control word is then re-encrypted at 95 using a recording key generated internally by the recorder security module and stored at 96. The new ECM comprising this re-encrypted control word and any other information is then recorded on the recording

support 97 together with the originally scrambled transmission. Upon playback of the recording, the recorder security module 52 will use the recording key value stored at 96 to decrypt the ECM so as to obtain the control word value to be used in decrypting the scrambled transmission prior to display.

In order to provide a safeguard copy, the recording key may be communicated to the decoder using the session key. The recording is thereafter stored in the decoder security module as a backup in the event of damage or loss of the recorder security module.

The private/public keys pairs KpriSIM, KpubSIM, KpriMan, KpubMan, KpriSystem and KpubSystem may be generated in accordance with any suitable asymmetric encryption algorithm such as RSA or Diffie-Hellman. Equally, the session key and recording key may correspond to key values usable with any suitable symmetric encryption/decryption algorithm such as DES.

As will be understood, alternative realisations of the above embodiment are possible. In the case, for example, where the same system manager is responsible for personalising managing both decoder and recorder security modules, the initial step of authentification using the system certificate CtKeyRec may be omitted, such that the value of KpubMan is directly inserted in the decoder module at 78.

Furthermore, in the case where the responsibility to ensure integrity of security of transmitted and recorded emissions rests with the manufacturer of the recorder, some or all of the roles of the decoder security module and recorder security module may be completely reversed, such that the recorder manufacturer certifies a public key provided by the broadcast system operator, the recorder is responsible for initiation of communication, generation of a session key etc.

In the same way, whilst the use of a changing session key increases the level of security, other realisations can be envisaged where a constant session key is used or where the public/private keys KpubSIM/KpriSIM are used to directly encrypt information communicated from the decoder to the recorder.

It will also be appreciated that, below the level of the generation of a session key, any number of possibilities for communication of information for use in recording may be envisaged. For example, whilst the data communicated from the decoder to the recorder comprises the control word in the described example it may be envisaged to decrypt and re-encrypt audiovisual data itself before communication to the recorder card. Alternatively, or in addition, the recording key may be generated at the decoder security module and communicated to the recorder security module.

Finally, whilst the above description has focused on the validation and communication of information in relation to single sources of recorders or decoders, the invention may equally expanded to cover multiple decoder and/or recorder sources. For example, a recorder security module may include a plurality of system certificates CtKeyRec associated with a plurality of broadcast system managers. Equally a decoder security module may be adapted to handle a plurality of recorder manufacturer management keys KpubMan obtained after the first verification step is carried out.

CLAIMS

1. A method of providing secure communication of information between a decoder device (12, 30) and a recorder device (50, 52) and characterised in that a first one of the devices communicates to the second device a certificate (CtKeySIM) comprising a device public key (KpubSIM) encrypted by a management private key (KpriMan), the second device decrypting the certificate using an equivalent management public key (KpubMan) and thereafter using the device public key (KpubSIM) to encrypt information sent to the first device, the first device using an equivalent device private key (KpriSIM) to decrypt the information.

2. A method as claimed in claim 1 in which the first device communicates to the second device a system certificate (CtKeyRec) comprising the management public key (KpubMan) encrypted by a system private key (KpriSystem), the second device decrypting the system certificate using a system public key (KpubSystem) so as to obtain the management public key (KpubMan) used thereafter to decrypt the device certificate (CtKeySIM).

3. A method as claimed in any preceding claim in which the device private/public key pair (KpriSIM, KpubSIM) are uniquely associated with the identity of the first device.

4. A method as claimed in any preceding claim in which the management private/public key pair (KpriMan, KpubMan) are uniquely associated with the source of the first device.

5. A method as claimed in claim 2 in which the system private/public key pair (KpriSystem, KpubSystem) are uniquely associated with the source of the second device.

6. A method as claimed in any preceding claim in which the encrypted information sent by the second device comprises a session key.

7. A method as claimed in claim 6 in which the session key is a key generated by the second device and usable in conjunction with a symmetric encryption algorithm.

8. A method as claimed in claim 6 or 7 in which the session key is used by the decoder device (12, 30) to encrypt control word information subsequently communicated to the recorder device (50, 52).

9. A method as claimed in claim 8 in which the recorder device (50, 52) may decrypt the control word information using the equivalent session key and thereafter re-encrypt the control word information using a recording encryption key, the re-encrypted control word information being stored by the recorder device (50, 52) on a recording support medium together with the scrambled transmission data associated with that control word information.

10. A method as claimed in claim 9 in which the recorder device (50, 52) communicates to the decoder device (12, 30) a copy of the recording encryption key.

11. A method as claimed in claim 10 in which the recorder device (50, 52) communicates a copy of the recording encryption key as encrypted by the session key.

12. A method as claimed in any preceding claim in which the recorder device (50, 52) and/or decoder device (12, 30) comprise one or more portable security modules (52; 30).

13. A method as claimed in any preceding claim in which the first device corresponds to a recorder device (50, 52) and the second device to a decoder device (12, 30).

14. A method as claimed in any preceding claim in which the decoder device (12, 30) is adapted to receive a digital television transmission.

Fig.1.

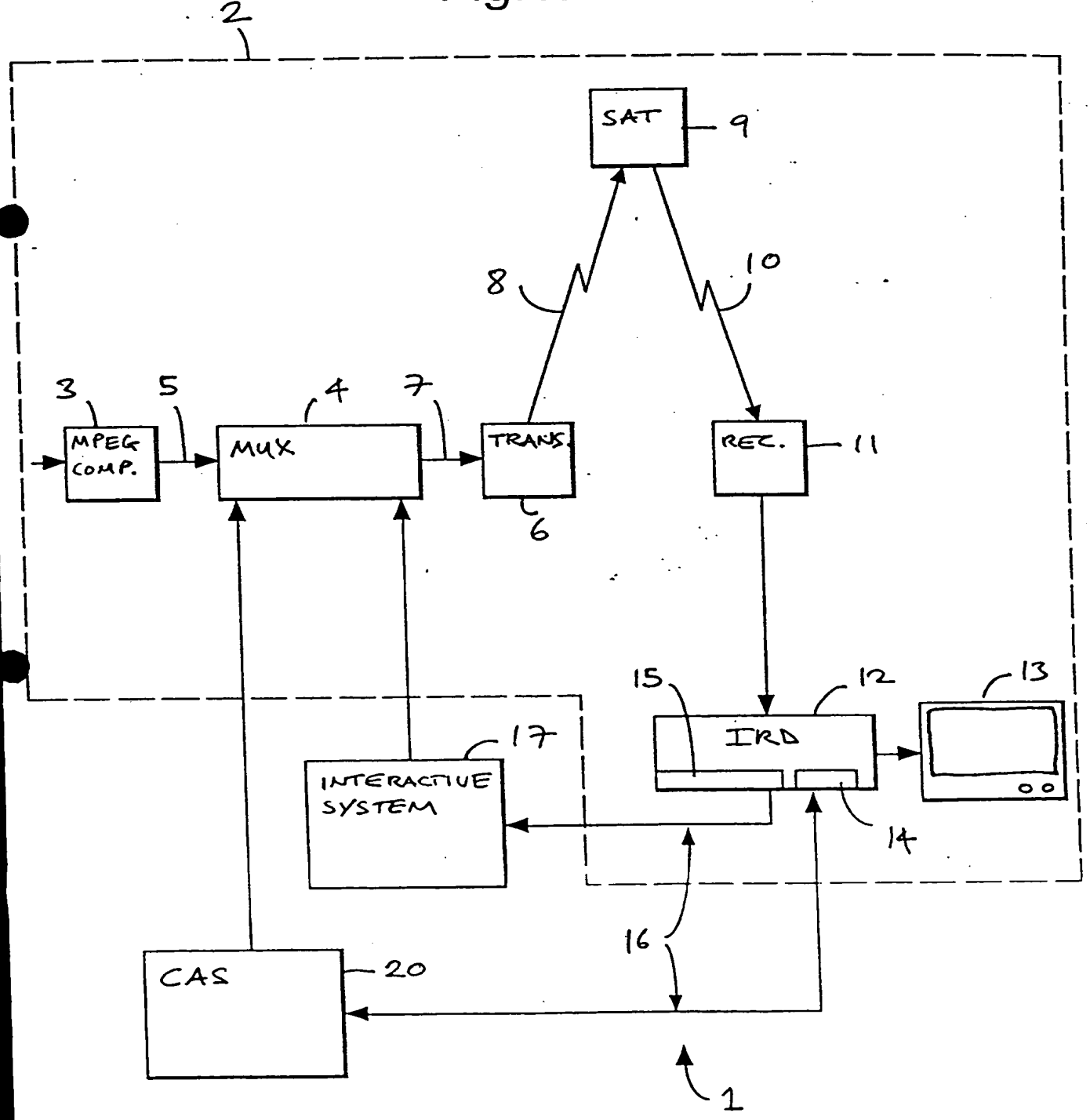

2
SAT
9
8
10
3
5
4
7
MPEG COMP.
MUX
TRANS.
REC.
11
6
15
12
13
IRD
17
INTERACTIVE SYSTEM
14
16
CAS
20
1

Fig.2.

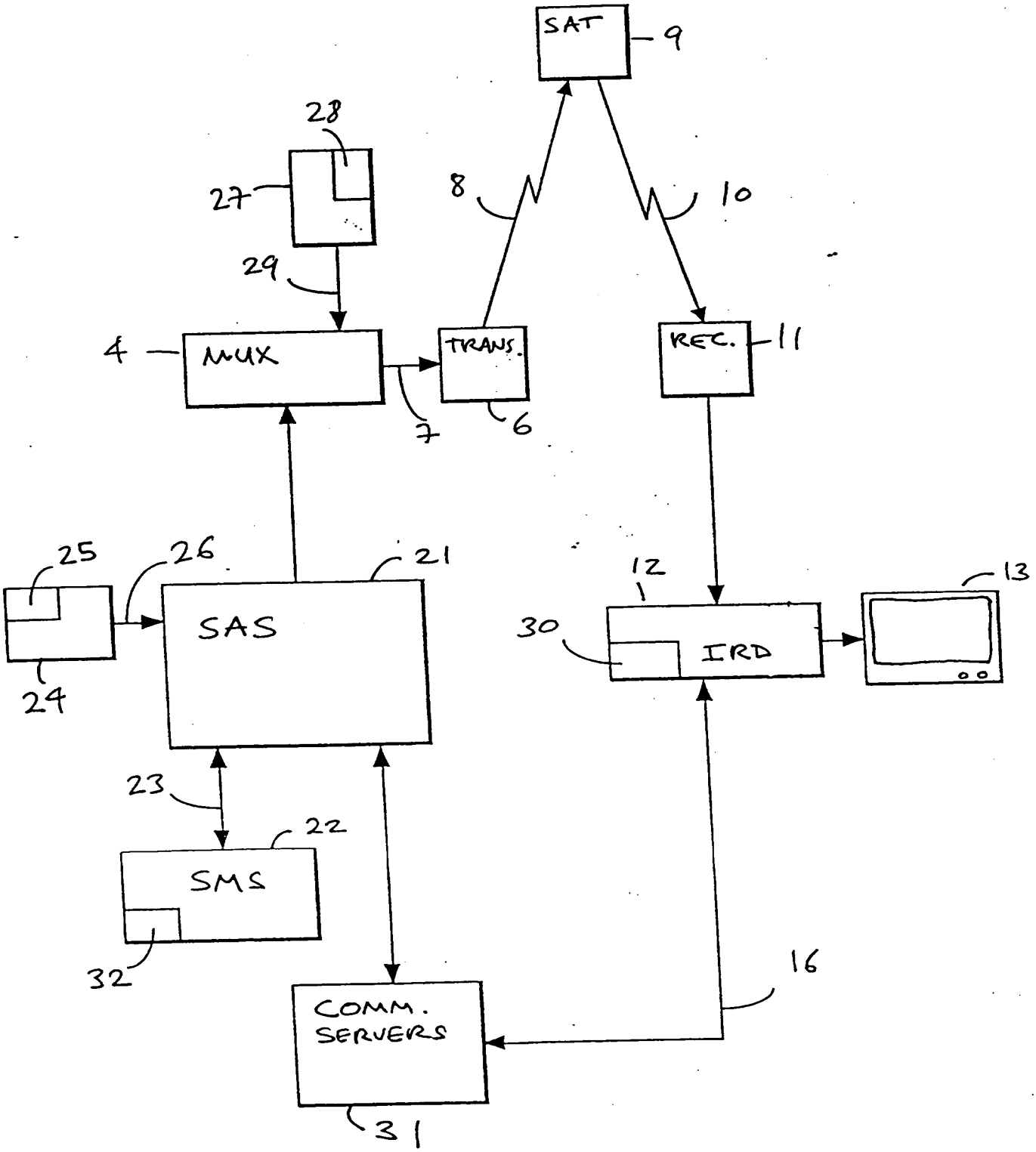
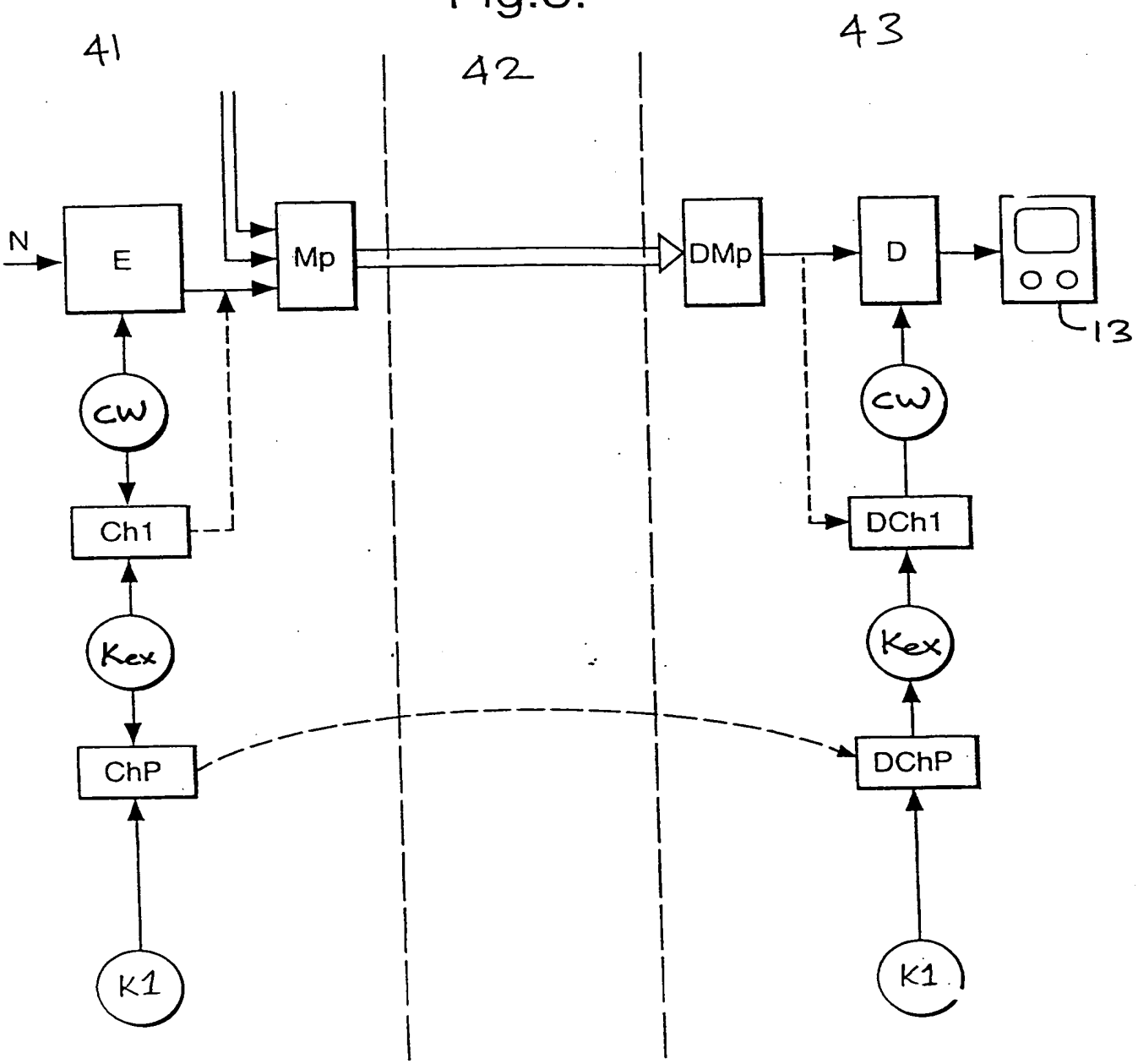

SAT
9
28
27
8
10
29
4
MUX
TRANS.
REC.
11
7
6
25
26
21
12
13
SAS
30
IRD
24
23
22
SMS
32
16
COMM.
SERVERS
31

Fig.3.


41
42
43
N
E
Mp
DMp
D
13
CW
Ch1
Kex
ChP
K1
CW
DCh1
Kex
DChP
K1

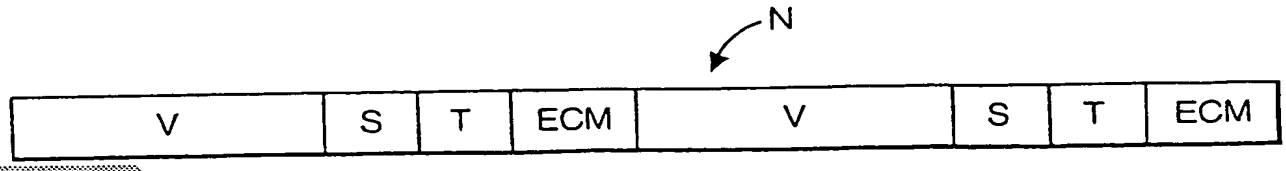

N
V
S
T
ECM
V
S
T
ECM

Figure 4

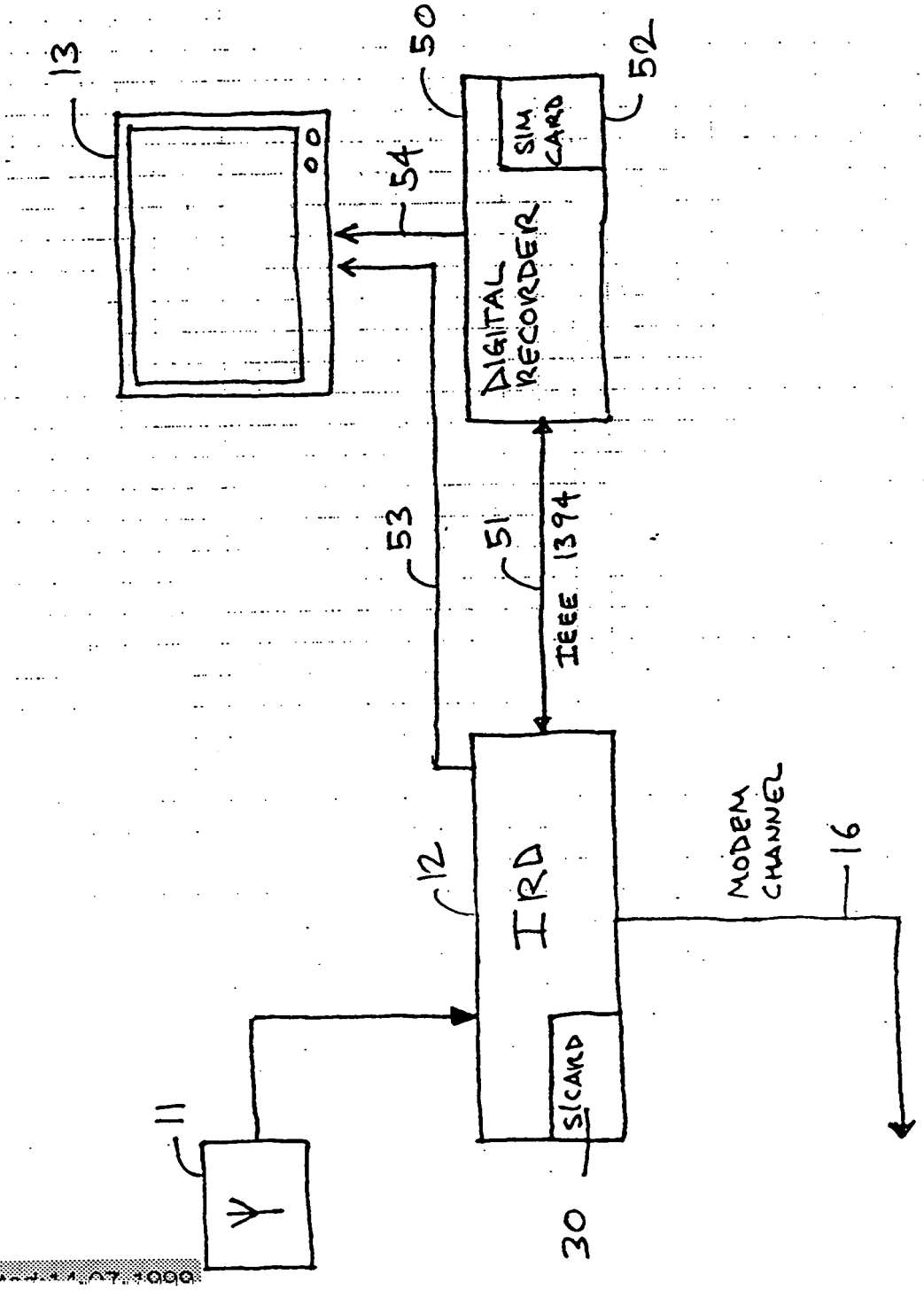
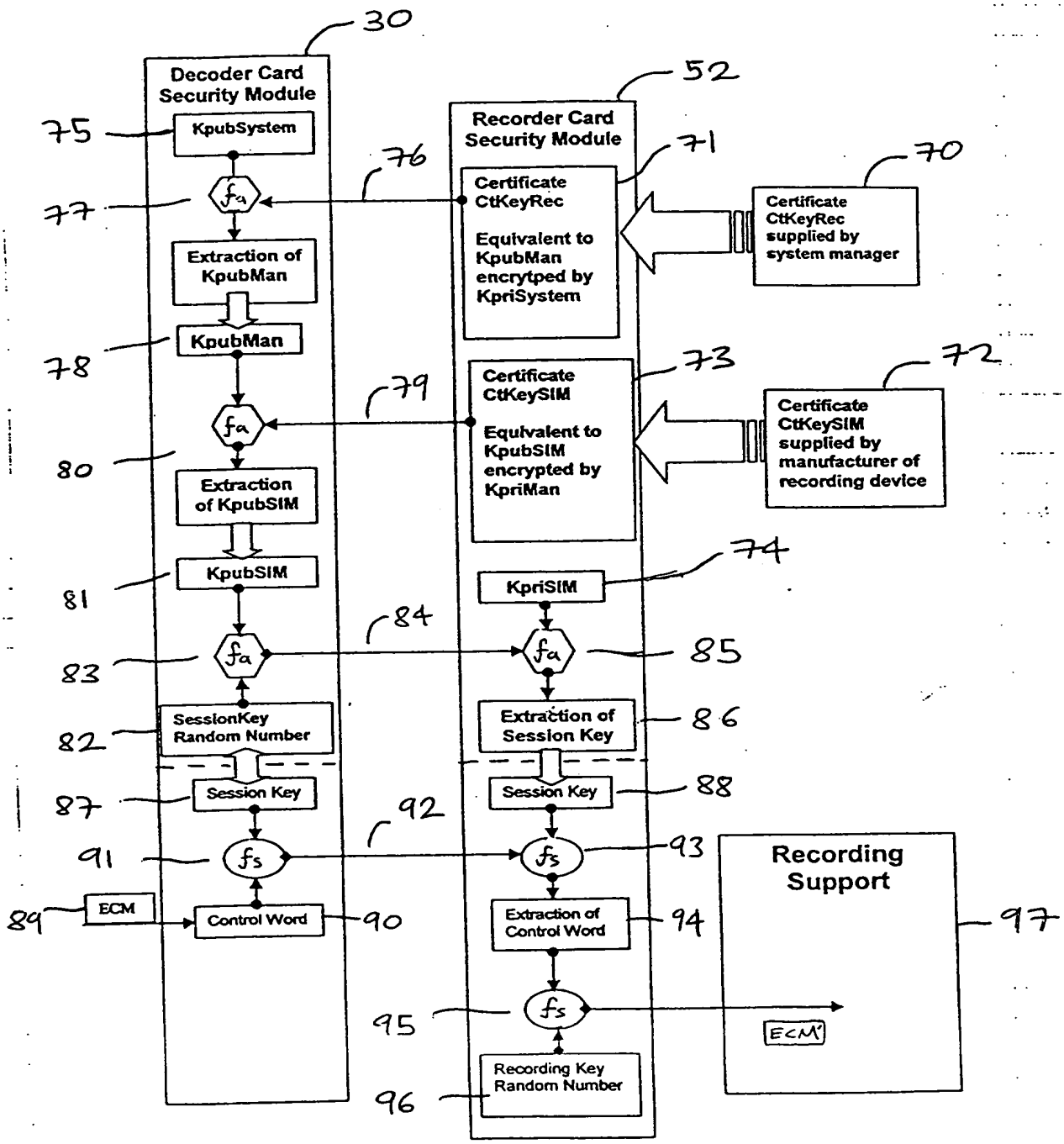

13
50
52
SIM CARD
54
DIGITAL RECORDER
53
51
IEEE 1394
12
IRD
MODEM CHANNEL
16
SICARD
30
11
Y

Figure 5


30
Decoder Card Security Module
52
Recorder Card Security Module
75
KpubSystem
76
71
70
Certificate CtKeyRec
Equivalent to KpubMan encrytped by KpriSystem
Certificate CtKeyRec supplied by system manager
77
fa
Extraction of KpubMan
KpubMan
78
79
73
72
Certificate CtKeySIM
Equivalent to KpubSIM encrypted by KpriMan
Certificate CtKeySIM supplied by manufacturer of recording device
80
Extraction of KpubSIM
KpubSIM
81
74
KpriSIM
84
83
85
SessionKey Random Number
82
Extraction of Session Key
86
Session Key
87
88
92
91
fs
93
Recording Support
89
ECM
Control Word
90
Extraction of Control Word
94
97
95
ECM
Recording Key Random Number
96

ABSTRACT

METHOD AND APPARATUS FOR SECURE COMMUNICATION OF INFORMATION BETWEEN A DECODER DEVICE AND A RECORDER DEVICE

A method of providing secure communication of information between a decoder device 30 and a recorder device 52 and characterised in that a first one of the devices 52 communicates to the second device 30 a certificate CtKeySIM comprising a device public key KpubSIM encrypted by a management private key KpriMan, the second device 30 decrypting the certificate using an equivalent management public key KpubMan and thereafter using the device public key KpubSIM to encrypt information sent to the first device 52, the first device 52 using an equivalent device private key KpriSIM to decrypt the information.

In a particularly preferred embodiment, the first device 30 communicates to the second device 52 a system certificate CtKeyRec comprising the management public key KpubMan encrypted by a system private key KpriSystem, the second device 30 decrypting the system certificate using a system public key KpubSystem so as to obtain the management public key KpubMan used thereafter to decrypt the device certificate CtKeySIM.

[Figure 5]